

# COMMONWEALTH OF VIRGINIA



## Information Technology Resource Management Guideline

### INTERNET PRIVACY GUIDELINES

Department of Technology Planning

## PREFACE

### PUBLICATION DESIGNATION

COV ITRM Guideline SEC2001-02.1

### SUBJECT

Public Body Internet Privacy Policy and Internet Privacy Policy Statement Guideline

### EFFECTIVE DATE

February 27, 2001

### SUPERSEDES

New

### SCHEDULED REVIEW

One (1) year from effective date

### AUTHORITY

Code of Virginia § 2.1-51.47

(Powers and Duties of the Secretary of Technology)

Code of Virginia § 2.1-51.48

(Powers and Duties of the Council on Technology Services)

Code of Virginia § 2.1-563.35:3

(Powers and Duties of the Department of Technology Planning)

Code of Virginia § 2.1-380

(Administration of systems including personal information; Internet privacy policy)

Executive Order 51 (99)

(Implementing Certain Recommendations by the Governor's Commission on Information Technology)

### SCOPE

This *guideline* is applicable to each public body that has an Internet website associated with that public body. It is optional for those public bodies with only Intranet websites.

Public bodies, as defined in Code of Virginia, §2.1-341, “means any legislative body; any authority, board, bureau, commission, district or agency of the Commonwealth or of any political subdivision of the Commonwealth, including cities, towns and counties; municipal councils, governing bodies of counties, school boards and planning commissions; boards of visitors of public institutions of higher education; and other organizations, corporations or agencies in the Commonwealth supported wholly or principally by public funds. It shall include any committee or subcommittee of the public body created to perform delegated functions of the public body or to advise the public body. It shall not exclude any such committee or subcommittee because it has private sector or citizen members. Corporations organized by the Virginia Retirement System are "public bodies" for purposes of this chapter.”

**PURPOSE**

To provide guidelines to public bodies with Internet websites for developing an Internet Privacy Policy and an Internet Privacy Policy Statement.

**GENERAL RESPONSIBILITIES****Secretary of Technology (SOTECH)**

The *Code of Virginia, §2.1-380*, "Administration of agency systems including personal information; Internet privacy policy," states that the Secretary of Technology, or his designee, shall provide guidelines for developing an Internet Privacy Policy and an Internet Privacy Policy Statement, and that each public body shall tailor the policy and the statement to reflect the information practices of the individual public body. SOTECH has designated the Department of Technology Planning as the agency to provide these guidelines.

**Secretary of Technology (SOTECH), Secretary of Administration (SOA), Council on Technology Services (COTS)**

*Executive Order 51 (99)* states, "The Secretary of Technology and the Secretary of Administration, working with the Council on Technology Services, shall jointly develop uniform guidelines for clear and explicit privacy policies and practices for agency Web sites."

**Department of Technology Planning (DTP)**

In accordance with the *Code of Virginia, §2.1-563.35:3*, the Department of Technology Planning is assigned the following duties: "To develop and promulgate policies, standards, and guidelines for managing information technology in the Commonwealth."

**Public Bodies**

Each public body, as defined in the *Code of Virginia, §2.1-341*, that has an Internet website associated with that public body shall develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public. The policy shall be consistent with the requirements of the *Code of Virginia, §2.1-380*. By January 1, 2001, the statement shall be made available on the public body's website in a conspicuous manner.

Each public body shall tailor the policy and the statement to reflect the information practices of the individual public body. At minimum, each public body's Internet Privacy Policy and Internet Privacy Policy Statement shall address (i) what information, including personally identifiable information, will be collected, if any; (ii) whether any information will be automatically collected simply by accessing the website and, if so, what information; (iii) whether the website automatically places a computer file, commonly referred to as a "cookie," on the Internet user's computer and, if so, for what purpose; and (iv) how the collected information is being used or will be used.

## TABLE OF CONTENTS

	<u>Page</u>
<b>PREFACE</b>	1
<b>TABLE OF CONTENTS</b>	3
<b>SECTION 1: INTRODUCTION</b>	
Purpose	4
Definition of a Guideline	4
Background	4
<b>SECTION 2: THE GUIDELINES</b>	
General Approach	5
Example Policy Statement	6
<b>APPENDICES</b>	
Appendix 1 – Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines	9
Appendix 2 - Virginia Privacy Protection Act of 1976	10

## SECTION 1

### INTRODUCTION

#### Purpose

To provide guidelines to public bodies with Internet websites for developing an Internet Privacy Policy and an Internet Privacy Policy Statement in accordance with Code of Virginia, §2.1-380 and Executive Order 65 (00). These guidelines are optional for websites maintained exclusively for use on Intranets.

#### Definition of a Guideline

Guidelines are directives and specifications, similar to standards, but advisory in nature. In essence, guidelines constitute recommendations that are not binding; however, it should be noted that parts of this guideline contain mandatory requirements from the Code of Virginia. Where that is the case, the terms “shall” or “must” are used.

#### Background

Virginia law requires that public bodies shall collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency. Virginia law also states that personal information shall not be collected unless the need for it has been clearly established in advance and that the personal information shall be appropriate and relevant to the purpose for which it has been collected. Virginia law further states that citizens should have access to public records and requires public bodies to provide copies of such records to requesting citizens, with certain specific exemptions.

When personal information is collected, there are specific requirements outlined in the “Virginia Privacy Protection Act of 1976” (Code of Virginia, § 2.1-377 – 386) which must be followed. (See Appendix 2.)

As defined in the Code of Virginia, §2.1-379, “The term “personal information” means all information that describes, locates or indexes anything about an individual, including his real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. The term does not include routine information maintained for the purpose of internal office administration, whose use could not be such as to affect adversely any data subject, nor does the term include real estate assessment information.”

## SECTION 2

### THE GUIDELINES

#### General Approach

1. Every public body that maintains an Internet website shall develop an Internet Privacy Policy and an Internet Privacy Policy Statement before December 1, 2000. The Internet Privacy Policy Statement shall be posted on the public body website before January 1, 2001.
2. Websites should be designed to collect only the minimum amount of information necessary for the public body to conduct its stated business. Internet servers do collect communication protocol addresses from the personal computers accessing the website in order to facilitate communication.
3. The Internet Privacy Policy and Internet Privacy Policy Statement shall explicitly state:
  - what information, including personally identifiable information, will be collected, if any;
  - whether any information will be automatically collected simply by accessing the website and, if so, what information;
  - whether the website automatically places a computer file, commonly referred to as a "cookie," on the Internet user's computer and, if so, for what purpose; and
  - how the collected information is being used or will be used.

Except for those systems exempt from the "Virginia Privacy Protection Act of 1976", as listed in the Code of Virginia, § 2.1-384, the following will also be included:

- a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination; and
  - a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information
4. The Internet Privacy Policy Statement, or a link to the Internet Privacy Policy Statement, will be featured in a conspicuous manner on the website home page, preferably at the top.
  5. The Internet Privacy Policy Statement shall also state that any personal information that is collected and retained is maintained in compliance with the "Virginia Privacy Protection Act of 1976", Code of Virginia, § 2.1-377 – 386, included as Appendix 2.
  6. Under the "Virginia Freedom of Information Act", citizens have the right to inspect and copy public records. The collection of logs and data of a website is a public record. The Internet Privacy Policy Statement will note this to remind users that the information that is collected may be provided to anyone that requests it under the "Virginia Freedom of Information Act".
  7. Modern information technology tools have the potential to extend the meaning of "personal information" to include the web browsing habits of users of the Internet. Web browsers have been designed with the ability to collect and pass potentially identifying

- information via “cookies” of which the user may not even be aware. Internet servers collect very specific information necessary to allow the transfer of information between computers. Until this issue is clarified, each public body should include a description of all types of data collected in their Internet Privacy Policy Statement.
8. Colleges and Universities that provide web hosting services for students will provide guidelines similar to those described above to their students and encourage their compliance.

### **Example Policy Statement**

*[Name of Public Body]*  
**Internet Privacy Policy Statement**  
*(last updated on [date])*

The following information explains the Internet Privacy Policy which the [name of public body] has adopted for its website (web pages at addresses beginning with "http://www.\_\_\_\_\_"). The following is intended to explain our current Internet privacy practices, but shall not be construed as a contractual promise. We reserve the right to amend our Internet Privacy Policy Statement at any time without notice.

#### **Virginia law**

We protect our records in accordance with our obligations as defined by applicable Virginia statutes, including, but not limited to, the “Virginia Privacy Protection Act of 1976”, the “Virginia Freedom of Information Act”, and by any applicable U.S. federal laws.

#### **Links to other websites**

Our website may contain links to other public or private entities' websites, whose privacy practices we do not control.

#### **Information we collect**

When you access our website, the routing or client information, and the essential and nonessential technical information listed below, is automatically collected. No other information is collected through our website except when you deliberately decide to send it to us (for example, by clicking on a link to send us an email). The information you might choose to send us is listed below as "optional information."

Routing, or client, information: the Internet domain and Internet address of the computer you are using.

Essential technical information: identification of the page or service you are requesting, type of browser and operating system you are using; and the date and time of access.

Nonessential technical information: the Internet address of the website from which you linked directly to our website [, and the "cookie information" described below].

Optional information: when you send us an e-mail, your name, e-mail address, and the content of your e-mail; when you fill out online forms, all the data you choose to fill in or confirm.

Cookies: Our website does not place any "cookies" on your computer.

- OR

[Our website places "cookies" on your computer, unless your browser is set to reject cookies. The cookies enable our website to recognize you when you return to the website at a later date or time and enables us to personalize the website with preferences or information you have provided during prior sessions. The cookie information placed on your computer by this website includes the following: \_\_\_\_\_.]

### **How the collected information is used**

Routing information is used to route the requested web page to your computer for viewing. We send the requested web page and the routing information to our Internet service provider or other entities involved in transmitting the requested page to you. We do not control the privacy practices of those entities. Essential and nonessential technical information helps us respond to your request in an appropriate format [or in a personalized manner] and helps us plan website improvements.

Optional information enables us to provide services or information tailored more specifically to your needs or to forward your message or inquiry to another entity that is better able to do so, and also allows us to plan website improvements.

We may keep your information indefinitely, but we ordinarily delete the transaction routing information from our computer within \_ days after the web page is transmitted and do not try to obtain any information to link it to the individuals who browse our website. However, on rare occasions when a "hacker" attempts to breach computer security, logs of routing information are retained to permit a security investigation and in such cases may be forwarded together with any other relevant information in our possession to law enforcement agencies. We use this transaction routing information primarily in a statistical summary type format to assess site content and server performance. We may share this summary information with our business partners when needed.

Optional information is retained in accordance with the records retention schedules at the Library of Virginia.

Under the "Virginia Freedom of Information Act", any records in our possession at the time of a "Freedom of Information Request" might be subject to being inspected by, or disclosed to, members of the public. However, all identifiable confidential/personal information will be removed prior to releasing the routing information.

### **Choice to provide information**

There is no legal requirement for you to provide any information at our website. However, our website will not work without routing information and the essential technical information. Failure of your browser to provide nonessential technical information will not prevent your use of our website, but may prevent certain features from working. Failure to provide optional

information will mean that the particular feature or service associated with that part of the web page will not be available to you.

**Customer comments or review**

If you have questions about this privacy statement or the practices of this website, or if you choose to review or correct any information you previously submitted, please contact us at \_\_\_\_\_ (e-mail address or phone number, etc.)

## **APPENDIX 1**

### **Assignment of Uniform Alphanumeric Publication Designations for all Policies, Standards, and Guidelines**

The Department of Technology Planning is responsible for assigning a uniform alphanumeric Publication Designation (PD) to all Commonwealth of Virginia (COV) Information Technology Resource Management (ITRM) Policies, Standards, and Guidelines (PSG). The PD is derived, in part, from components of the Commonwealth Enterprise Architecture (EA) known as “Infrastructure Domains.” The “Infrastructure Domains” and Governance are defined in the [Commonwealth EA Glossary](#). The Governance code is used to identify those PSG that are not uniquely related to a specific infrastructure domain, e.g. “IT Project Management” or “IT Project Oversight.”

The following alpha codes will be used to identify each PSG:

#### **Infrastructure Domains + Governance**

#### **Code**

Governance and Transitional Processes	GOV
Platform Architecture	PLA
Database Architecture	DAT
Network Architecture	NET
Security Architecture	SEC
Cost Allocation Architecture	COS
Systems Management Architecture	SYS
Information Architecture	INF
Application Architecture	APP
Middleware Architecture	MID

Publication Designations are constructed as follows:

COV ITRM (“Policy,” “Standard,” or “Guideline”) XXXYYYY-ZZZ

Where:       XXX is the assigned Infrastructure Domain + Governance code;  
              YYYY is the year of initial issue; and  
              ZZZ is the sequential number assigned to link related PSG

Example:       COV ITRM Standard GOV2000-01.1 is a Standard that implements  
              COV ITRM Policy GOV2000-01.1

**APPENDIX 2**

The Internet Privacy Policy Statement should state that any personal information that is collected and retained is maintained in compliance with the “Virginia Privacy Protection Act of 1976”, *Code of Virginia, § 2.1-377 – 386*. It is recommended that applicable sections of the code be inserted in the policy statement.

**“Virginia Privacy Protection Act of 1976”**

§ 2.1-377. Short title.

This chapter may be cited as the "Privacy Protection Act of 1976."

§ 2.1-378. Findings; principles of information practice.

A. The General Assembly finds:

1. That an individual's privacy is directly affected by the extensive collection, maintenance, use and dissemination of personal information;

2. That the increasing use of computers and sophisticated information technology has greatly magnified the harm that can occur from these practices;

3. That an individual's opportunities to secure employment, insurance, credit and his right to due process, and other legal protections are endangered by the misuse of certain of these personal information systems; and

4. That in order to preserve the rights guaranteed a citizen in a free society, legislation is necessary to establish procedures to govern information systems containing records on individuals.

B. Record-keeping agencies of the Commonwealth and political subdivisions shall adhere to the following principles of information practice to ensure safeguards for personal privacy:

1. There shall be no personal information system whose existence is secret.

2. Information shall not be collected unless the need for it has been clearly established in advance.

3. Information shall be appropriate and relevant to the purpose for which it has been collected.

4. Information shall not be obtained by fraudulent or unfair means.

5. Information shall not be used unless it is accurate and current.

6. There shall be a prescribed procedure for an individual to learn the purpose for which information has been recorded and particulars about its use and dissemination.

7. There shall be a clearly prescribed and uncomplicated procedure for an individual to correct, erase or amend inaccurate, obsolete or irrelevant information.

8. Any agency holding personal information shall assure its reliability and take precautions to prevent its misuse.

9. There shall be a clearly prescribed procedure to prevent personal information collected for one purpose from being used for another purpose.

10. The Commonwealth or any agency or political subdivision thereof shall not collect personal information except as explicitly or implicitly authorized by law.

§ 2.1-379. Definitions.

As used in this chapter:

1. The term "information system" means the total components and operations of a record-keeping process, including information collected or managed by means of computer networks and the global information system known as the Internet, whether automated or manual, containing personal information and the name, personal number, or other identifying particulars of a data subject.

2. The term "personal information" means all information that describes, locates or indexes anything about an individual including his real or personal property holdings derived from tax returns, and his education, financial transactions, medical history, ancestry, religion, political ideology, criminal or employment record, or that affords a basis for inferring personal characteristics, such as finger and voice prints, photographs, or things done by or to such individual; and the record of his presence, registration, or membership in an organization or activity, or admission to an institution. The term does not include routine information maintained for the purpose of internal office administration whose use could not be

such as to affect adversely any data subject nor does the term include real estate assessment information.

3. The term "data subject" means an individual about whom personal information is indexed or may be located under his name, personal number, or other identifiable particulars, in an information system.

4. The term "disseminate" means to release, transfer, or otherwise communicate information orally, in writing, or by electronic means.

5. The term "purge" means to obliterate information completely from the transient, permanent, or archival records of an organization.

6. The term "agency" means any agency, authority, board, department, division, commission, institution, bureau, or like governmental entity of the Commonwealth or of any unit of local government including counties, cities, towns and regional governments and the departments and including any entity, whether public or private, with which any of the foregoing has entered into a contractual relationship for the operation of a system of personal information to accomplish an agency function. Any such entity included in this definition by reason of a contractual relationship shall only be deemed an agency as relates to services performed pursuant to that contractual relationship, provided that if any such entity is a consumer reporting agency, it shall be deemed to have satisfied all of the requirements of this chapter if it fully complies with the requirements of the Federal Fair Credit Reporting Act as applicable to services performed pursuant to such contractual relationship.

§ 2.1-380. Administration of systems including personal information; Internet privacy policy.

A. Any agency maintaining an information system that includes personal information shall:

1. Collect, maintain, use, and disseminate only that personal information permitted or required by law to be so collected, maintained, used, or disseminated, or necessary to accomplish a proper purpose of the agency;

2. Collect information to the greatest extent feasible from the data subject directly;

3. Establish categories for maintaining personal information to operate in conjunction with confidentiality requirements and access controls;

4. Maintain information in the system with accuracy, completeness, timeliness, and pertinence as necessary to assure fairness in determinations relating to a data subject;

5. Make no dissemination to another system without (i) specifying requirements for security and usage including limitations on access thereto and (ii) receiving reasonable assurances that those requirements and limitations will be observed, provided this subdivision shall not apply to a dissemination made by an agency to an agency in another state, district or territory of the United States where the personal information is requested by the agency of such other state, district or territory in connection with the application of the data subject therein for a service, privilege or right under the laws thereof, nor shall this apply to information transmitted to family advocacy representatives of the United States Armed Forces in accordance with subsection O of § [63.1-248.6](#);

6. Maintain a list of all persons or organizations having regular access to personal information in the information system;

7. Maintain for a period of three years or until such time as the personal information is purged, whichever is shorter, a complete and accurate record, including identity and purpose, of every access to any personal information in a system, including the identity of any persons or organizations not having regular access authority but excluding access by the personnel of the agency wherein data is put to service for the purpose for which it is obtained;

8. Take affirmative action to establish rules of conduct and inform each person involved in the design, development, operation, or maintenance of the system, or the collection or use of any personal information contained therein, about all the requirements of this chapter, the rules and procedures, including penalties for noncompliance, of the agency designed to assure compliance with such requirements;

9. Establish appropriate safeguards to secure the system from any reasonably foreseeable threat to its security; and

10. Collect no personal information concerning the political or religious beliefs, affiliations, and activities of data subjects which is maintained, used or disseminated in or by any information system operated by any agency unless authorized explicitly by statute or ordinance.

B. By December 1, 2000, every public body, as defined in § [2.1-341](#), that has an Internet website associated with that public body shall develop an Internet privacy policy and an Internet privacy policy statement that explains the policy to the public. The policy shall be consistent with the requirements of this chapter. By January 1, 2001, the statement shall be made available on the public body's website in a conspicuous manner. The Secretary of Technology or his designee shall provide guidelines for developing the policy and the statement, and each public body

shall tailor the policy and the statement to reflect the information practices of the individual public body. At minimum, the policy and the statement shall address (i) what information, including personally identifiable information, will be collected, if any; (ii) whether any information will be automatically collected simply by accessing the website and, if so, what information; (iii) whether the website automatically places a computer file, commonly referred to as a "cookie," on the Internet user's computer and, if so, for what purpose; and (iv) how the collected information is being used or will be used.

§ 2.1-380.1. Same; military recruiters to have access to student information, school buildings, etc.

If a public school board or public institution of higher education provides access to its buildings and grounds and the student information directory to persons or groups which make students aware of occupational or educational options, the board or institution shall provide access on the same basis to official recruiting representatives of the military forces of the Commonwealth and the United States for the purpose of informing students of educational and career opportunities available in the military.

§ 2.1-381. Same; dissemination of reports.

Any agency maintaining an information system that disseminates statistical reports or research findings based on personal information drawn from its system, or from other systems shall:

1. Make available to any data subject or group, without revealing trade secrets, methodology and materials necessary to validate statistical analysis, and
2. Make no materials available for independent analysis without guarantees that no personal information will be used in any way that might prejudice judgments about any data subject.

§ 2.1-382. Rights of data subjects.

A. Any agency maintaining personal information shall:

1. Inform an individual who is asked to supply personal information about himself whether he is legally required, or may refuse, to supply the information requested, and also of any specific consequences which are known to the agency of providing or not providing such information.
2. Give notice to a data subject of the possible dissemination of part or all of this information to another agency, nongovernmental organization or system not having regular access authority, and indicate the use for which it is intended, and the specific consequences for the individual, which are known to the agency, of providing or not providing

such information, however documented permission for dissemination in the hands of such other agency or organization will satisfy this requirement. Such notice may be given on applications or other data collection forms prepared by data subjects.

3. Upon request and proper identification of any data subject, or of his authorized agent, grant such subject or agent the right to inspect, in a form comprehensible to such individual or agent:

(a) All personal information about that data subject except as provided in § 2.1-342 B 3.

(b) The nature of the sources of the information.

(c) The names of recipients, other than those with regular access authority, of personal information about the data subject including the identity of all persons and organizations involved and their relationship to the system when not having regular access authority, except that if the recipient has obtained the information as part of an ongoing criminal investigation such that disclosure of the investigation would jeopardize law-enforcement action, then no disclosure of such access shall be made to the data subject.

4. Comply with the following minimum conditions of disclosure to data subjects:

(a) An agency shall make disclosures to data subjects required under this chapter, during normal business hours.

(b) The disclosures to data subjects required under this chapter shall be made (i) in person, if he appears in person and furnishes proper identification, or (ii) by mail, if he has made a written request, with proper identification. Copies of the documents containing the personal information sought by a data subject shall be furnished to him or his representative at reasonable standard charges for document search and duplication.

(c) The data subject shall be permitted to be accompanied by a person or persons of his choosing, who shall furnish reasonable identification. An agency may require the data subject to furnish a written statement granting permission to the organization to discuss the individual's file in such person's presence.

5. If the data subject gives notice that he wishes to challenge, correct, or explain information about him in the information system, the following minimum procedures shall be followed:

(a) The agency maintaining the information system shall investigate, and record the current status of that personal information.

(b) If, after such investigation, such information is found to be incomplete, inaccurate, not pertinent, not

timely, or not necessary to be retained, it shall be promptly corrected or purged.

(c) If the investigation does not resolve the dispute, the data subject may file a statement of not more than 200 words setting forth his position.

(d) Whenever a statement of dispute is filed, the organization maintaining the information system shall supply any previous recipient with a copy of the statement and, in any subsequent dissemination or use of the information in question, clearly note that it is disputed and supply the statement of the data subject along with the information.

(e) The agency maintaining the information system shall clearly and conspicuously disclose to the data subject his rights to make such a request.

(f) Following any correction or purging of personal information the agency shall furnish to past recipients notification that the item has been purged or corrected whose receipt shall be acknowledged.

B. Nothing in this section or found elsewhere in this chapter shall be construed so as to require an agency to disseminate any recommendation or letter of reference from or to a third party which is a part of the personnel file of any data subject nor to disseminate any test or examination used, administered or prepared by any public body for purposes of evaluation of (i) any student or any student's performance, (ii) any seeker's qualifications or aptitude for employment, retention, or promotion, or (iii) qualifications for any license or certificate issued by any public body.

As used in this subsection, "test or examination" shall include (i) any scoring key for any such test or examination and (ii) any other document which would jeopardize the security of such test or examination. Nothing contained in this subsection shall prohibit the release of test scores or results as provided by law, or to limit access to individual records as is provided by law; however, the subject of such employment tests shall be entitled to review and inspect all documents relative to his performance on such employment tests.

When, in the reasonable opinion of such public body, any such test or examination no longer has any potential for future use, and the security of future tests or examinations will not be jeopardized, such test or examination shall be made available to the public. Minimum competency tests administered to public school children shall be made available to the public contemporaneously with statewide release of the scores of those taking such tests, but in no event shall such tests be made available to the public later than six months after the administration of such tests.

C. Neither any provision of this chapter nor any provision of Chapter 21 (§ [2.1-340](#) et seq.) of this title shall be construed as denying public access to records

of the position, job classification, official salary or rate of pay of, and to records of the allowances or reimbursements for expenses paid to any public officer, official or employee at any level of state, local or regional government in this Commonwealth whatsoever. The provisions of this subsection shall not apply to records of the official salaries or rates of pay of public employees whose annual rate of pay is \$10,000 or less.

D. Nothing in this section or in this chapter shall be construed to require an agency to disseminate information derived from tax returns in violation of §§ 2.1-342 and 58.1-3.

§ 2.1-383. Agencies to report concerning systems operated or developed; publication of information.

Every agency shall make report of the existence of any information system which it operates or develops which will include a description of the nature of the data in the system and purpose for which it is used. An inventory listing or similar display of such information shall be made available for inspection by the general public in the office of the head of each agency. Copies of such information shall be provided upon request and a fee shall be charged for the same sufficient to cover the reasonable costs of reproduction.

§ 2.1-384. Systems to which chapter inapplicable.

The provisions of this chapter shall not be applicable to personal information systems:

1. Maintained by any court of this Commonwealth;
2. Which may exist in publications of general circulation;
3. Contained in the Criminal Justice Information System as defined in §§ [9-184](#) through [9-196](#);
4. Contained in the Virginia Juvenile Justice Information System as defined in §§ [16.1-222](#) through [16.1-225](#);
5. Maintained by agencies concerning persons required to be licensed by law in this Commonwealth to engage in the practice of any professional occupation, in which case the names and addresses of persons applying for or possessing any such license may be disseminated upon written request to a person engaged in the profession or business of offering professional educational materials or courses for the sole purpose of providing such licensees or applicants for licenses with informational materials relating solely to available professional educational materials or courses, provided such disseminating agency is reasonably assured that the use of such information will be so limited;

6. Maintained by the Parole Board, the Crime Commission, the Judicial Inquiry and Review Commission and the Department of Alcoholic Beverage Control;

7. Maintained by the Department of State Police; police departments of cities, counties, and towns; and the campus police departments of public institutions of higher education as established by Chapter 17 (§ [23-232](#) et seq.) of Title 23, and which deal with investigations and intelligence gathering relating to criminal activity; and maintained by local departments of social services regarding alleged cases of child abuse or neglect while such cases are also subject to an ongoing criminal prosecution;

8. Maintained by the Virginia Port Authority as provided in § [62.1-134.1](#) or § [62.1-132.4](#);

9. Maintained by the Virginia Economic Development Partnership in connection with or as a result of the promotion of travel or tourism in the Commonwealth, in which case names and addresses of persons requesting information on those subjects may be disseminated upon written request to a person engaged in the business of providing travel services or distributing travel information, provided the Virginia Economic Development Partnership is reasonably assured that the use of such information will be so limited;

10. Maintained by the Division of Consolidated Laboratory Services of the Department of General Services and the Division of Forensic Science of the Department of Criminal Justice Services, which deal with scientific investigations relating to criminal activity or suspected criminal activity, except to the extent that § [9-196.11](#) may be applicable;

11. Maintained by the Department of Corrections which deal with investigations and intelligence gathering by persons acting under the provisions of § [53.1-16](#); and

12. Maintained by the Department of the State Internal Auditor or internal audit departments of state agencies or institutions which deal with communications and investigations relating to the State Employee Fraud, Waste and Abuse Hotline.

§ 2.1-384.1. Exception for state retirement systems.

Notwithstanding the provisions of § [2.1-380](#), the Virginia Retirement System may disseminate information as to the retirement status or benefit eligibility of any employee covered by the Virginia Retirement System, the Judicial Retirement System, the State Police Officers' Retirement System, or the Virginia Law Officers' Retirement System, to the chief executive officer or personnel officers of the state or local agency by which he is employed.

§ 2.1-385. Disclosure of social security number.

On or after July 1, 1977, it shall be unlawful for any agency to require an individual to disclose or furnish his social security account number not previously disclosed or furnished, for any purpose in connection with any activity, or to refuse any service, privilege or right to an individual wholly or partly because such individual does not disclose or furnish such number, unless the disclosure or furnishing of such number is specifically required by federal or state law.

§ 2.1-386. Injunctive relief.

Any aggrieved person may institute a proceeding for injunction or mandamus against any person or agency which has engaged, is engaged, or is about to engage in any acts or practices in violation of the provisions of this chapter. The proceeding shall be brought in the circuit court of any county or city wherein the person or agency made defendant resides or has a place of business. In the case of any successful proceeding by an aggrieved party, the person or agency enjoined or made subject to a writ of mandamus by the court shall be liable for the costs of the action together with reasonable attorney's fees as determined by the court.

